Bulgaria: The Rise And Decline Of Bulgaria's Interest In Information Operations

By Dr. Todor Tagarev

Editorial Abstract: Dr. Todor Tagarev described Bulgaria's need to build selective IO capabilities that assist in the conduct of NATO's effects-based operations. In particular he recommends Bulgaria should work to define generic units that are relatively self-sustained and can bring useful capabilities to a multinational operation. Bulgaria is also exploring what specialties it can contribute to the European Union with regard to critical infrastructure protection, where it hopes to remain competitive and capable of providing useful contributions.

Opinions expressed are solely those of the author and do not reflect official positions of the G.S. Rakovski Defense and Staff College, the Ministry of Defense of the Republic of Bulgaria, or any other governmental institution.

Introduction

At the beginning of the 1990s the Bulgarian military found itself in a void. The country had no paradigm that would facilitate the post-Cold war transition, and no one in the old or emerging leadership had experience in devising national security and defense policies. The armed forces enjoyed very high prestige in the eyes of the people, who were—and still are—proud of Bulgaria's military traditions.

While a member of the Warsaw Pact, Bulgaria was part of a very highly centralized system of force planning and conceptualization. The officer corps was well trained and very efficient in following Warsaw Pact (i.e. Soviet) doctrine, operational concepts, and tactics, but had minor (if any) contribution to force planning and the development of innovative concepts of operations. Thus, Bulgaria lacked officers with experience to generate doctrine, force structure, and concepts of operations to fit the requirements of the new security environment. In addition, until the end of the 1990s there was no civilian expertise on defense matters, neither in the executive branch nor in parliament. Not surprisingly, from 1990 until 1998 Bulgaria adhered to its "inherited" force structure, while its military organization evolved primarily under the pressures of rapidly declining defense budgets.

In such a situation the institutes within the Ministry of Defense that may have otherwise been instrumental in devising operational concepts, adequate to meet the changing threat, technological, and business environment, did not respond to the challenge. On the contrary, research organizations were among the first to suffer from budget cuts resulting in a brain drain. Nevertheless, around the mid-1990s a few curious Bulgarian officers, on their own initiative, decided to study information warfare and information operations developments and were able to attract the attention of the senior military leadership. Based on this, Bulgaria adopted a comprehensive set of new doctrinal documents from 1999 through 2002. The first part of this essay examines the respective developments and outlines the country's understanding of information operations and its component parts. The second part briefly addresses Bulgaria's approach to the neutralization of the extremist's use of the Internet. The final part of the essay examines the need to incorporate innovative operational thinking in the force planning process, and explains the reasons behind the decline of Bulgaria's interest in information operations. The essay concludes with a reiteration of the necessity to build selective capabilities for conducting information operations as a component of the NATO Effects-Based Approach to Operations (EBAO) and related developments within the European Security and Defense Policy—a necessity that may be met through a more realistic policy and efficient capability management. It is possible (and appropriate) to examine other component parts of information operations such as the security of information and command and control systems (for the military) and critical information infrastructure protection measures for the civilian sector.

Bulgarian soldier raises his national colors during a NATO exercise. (Defense Link)

Bulgaria's View of IO

The impressive utilization of advanced communications, information, sensors, and navigation technologies by the US military during the First Gulf War, 1990-1991, allowed the US-led coalition to achieve quick and decisive victory over Iraq. This placed information warfare among the top research topics for defense establishments around the world. But in Bulgaria, given the overwhelming problems in dealing with a Cold War force structure and size under declining budgets, the official defense establishment was not able to react properly.

Fortunately, as early as 1992 Bulgarian officers got the chance to study in Western military colleges, and rapid access to Internet sources provided information at previously unthinkable ease and speed. The combination of these two factors, plus the process of democratization of Bulgarian society enhanced the opportunities for curious individuals to collect information, analyze, synthesize, and reach broad audiences. Thus, in the mid-1990s, a venture of individual researchers with professional interests in military affairs and in particular the link between advances in IT and warfare, culminated in the publication of the book *Information Aspects of Security*.

The authors of this book examined a series of issues: the relationship between security and IT developments; conflicts related to the emergence of an information society; the main technologies providing for a competitive edge in information age conflicts; and main issues in managing the information environment. Of particular importance for this essay is the examination of information warfare—its principles, levels, domains, and components. In the book, Velizar Shalamanov and this author define information warfare as: a system of actions undertaken in order to create information space, in which one side has superior understanding and use of strong and weak points in the political, economic, military, social, and cultural domains of activity of a potential enemy and its dependence on friendly sources of power, and at the same time does not allow effective enemy actions. The authors identified information as a distinct domain, powerful weapon, and lucrative target in the evolution of conflict. They defined the term "information power" as the capacity created by advanced technologies, procedures, and organization. Further, they define the information campaign as the main tool, used in combination with traditional military means and approaches, to achieve information superiority, and distinguished two levels of this campaign:

- A strategic information campaign which ideally tried to achieve paralysis of the OODA-loop of the opponent;
- Command and control warfare campaign which supported strategic objectives through effects against the ability of the enemy to make timely and effective decisions on the use of its armed forces.

According to Shalamanov and Tagarev, the operation for achieving information superiority has six elements:

1. Security of operations—not allowing the enemy to receive adequate information on us; includes communications security, computer security, emission control, etc.;
2. Deception;
3. Psychological operations;
4. Electronic Warfare;
5. Physical effects on enemy C4ISR systems;
6. Superior situational awareness through the fusion of all-source intelligence

In addition, the authors examined the offensive and defensive aspects of information operations, the role of the media, and information aspects of operations other than war. Importantly, in a forward to that book General Miho Mihov—at the time a three-star equivalent and Chief of Staff of the Air Force and later (1997-2002) Chief of the General Staff of the Bulgarian Armed Forces—presented his views on the role of information in modern conflict. The following is a brief summary of his main points:

- Warfare has moved out of traditional domains and into the information domain;
- Information superiority is the means that may dissuade an opponent, postpone aggression, and even prevent a war;
- Winning the information war predefines the outcome of "classic" military activities;
- A new balance must be found between information power and firepower;
- The country has no alternative, but to prepare for information war.

A series of articles by the *Information Aspects of Security* authors, in the Bulgarian Ministry of Defense/Bulgarian Armed Forces official theoretical publication *Voenen Journal*, raised IWs awareness among Bulgarian security and defense experts. Further, it facilitated the debate on possible objectives in the utilization of advanced IT under new operational concepts, and the balance of priorities in the development of the armed forces.

In 1998, on the wave of rising interest in the relationships among security, warfare, and technology, the authors began publication of *Information & Security: An International Journal* with the intention to cover "scientific, technical, and policy issues related to national and international security in the Information Age, C4ISR technologies and systems, information operations, command and control warfare, and information assurance." The journal's stated objective is "to bridge the IT and the security communities, presenting state of the art, new findings, ideas, and needs of one community versus the other, as well as to present the latest research conducted 'on the bridge' between the two communities."

General Mihov—already Chief of the General Staff of the Bulgarian Armed Forces—contributed an article to the *Information & Security* pilot issue, conceptualizing in the context of the reform of the Bulgarian Armed Forces, and examining information warfare on the strategic and operational levels. He further reasoned that information operations were turning into a main supporting operation, and in the future, would be a distinct operation of the armed forces, to be conducted jointly with other governmental and public organizations. Paraphrasing the definition proposed by Shalamanov and Tagarev, General Mihov defined the term information operation as: a system of actions for the creation of an information space, in which one side has superiority in understanding and using the strong and weak aspects in the political, economic, military, ecological, social, and cultural areas of activity of a potential enemy and its dependence on friendly sources of power, while at the same time not allowing identical activities on its side.

He saw the objective of the information operation as "changing the way of reasoning and decision making of the enemy in the direction of our interests." General Mihov defined the term "information superiority" and linked information operations with other activities of the armed forces.

Coincidentally, all three Bulgarian authors mentioned so far played key roles in the development of the first national military doctrine: General Mihov as Chief of the General Staff; Dr. Shalamanov as Deputy Minister of Defense for defense policy and planning; and this author as a civilian Director for Defense Planning in the Ministry of Defense. The *Military Doctrine* was the first official document treating the issue of information operations and other information aspects of security. For example, the doctrine lists "information war/warfare" among the modern risks to security (articles 9, 11), and states the military threat to the country may be expressed, inter alia, via information attacks of another state against 'national strategic systems' (article 16). For the first time, it set achievement of information superiority as a military task. According to article 62, "the armed forces protect the country through the application of a military-strategic concept for defense of the national territory, a struggle for information superiority, control of the air and sea space, and defense of a threatened theater of military activities." Respectively, the doctrine defined as the priorities in the [technological] modernization of the armed forces "the C4ISR, identification and navigation … systems, the means and technologies to provide for interoperability with the armed forces of NATO countries, and the transition to an information society" (article 97).

The *Military Strategy*—a follow-up document—reiterated many of the postulates of the military doctrine, including its Article 62. Additionally, it listed the "reliable provision of information" among the main requirements towards the reform of the armed forces and defined the "strategic defensive operation" as a joint operation of the country's armed forces that includes, inter alia, information operations.

Bulgaria produced a number of additional doctrinal documents between 1999 and 2002. The 2001 *Joint Operations Doctrine* shed further light on official views of information operations. For example, the title of Section 5 in the chapter "Joint Operations in Armed Conflict" is "Information Operations" with the subtitle "Operations against C4I systems." It defined information operations as "a set of information effects, attacks, and battles, with coordinated objectives, tasks, place and time, conducted according to a distinct design and plan for solving the tasks of an information battle in the theater of military activities or on an operational direction." It states that IOs support strategic objectives through their influence on the ability of an enemy to make timely and effective decisions on the use of its armed forces. The doctrine defines two component parts of IO as well as other realms:

• Defensive—protecting the effectiveness of our own C2 system;

• Effecting – influencing, damaging, and destroying the enemy's C2;

• Other IO realms;

• Security operations;

• Disinformation (with a set of measures on the strategic, operational, and tactical levels);

• Psychological operations;

• Electronic Warfare.

Further, the doctrine designates the J3 staff as responsible for planning and coordinating the conduct of security operations, disinformation, psychological operations, and operations against the enemy's C2 systems, and the J6 staff for organizing the protection of information.

The 2002 *Air Force Doctrine* delineates between 'subordinated' and 'supporting' operations, with special operations and operations against C2 systems being part of the latter. As components of operations against C2 systems it lists security operations, psychological operations, disinformation, and electronic warfare. It assigns the air force a number of tasks, including countering an enemy's command and control, aerial intelligence, and 'special activities in the interest of information superiority.'

The 2002 *Land Forces Doctrine* includes a requirement that the Special Operations Forces are trained to participate in psychological operations and to support information operations.

The *Main Guidance to Operations Planning*, issued in 2000, followed the respective NATO documents and included requirements for two annexes to plans of operations (in addition to the more traditional ones)—on Psychological Operations and on Information Operations.

The publications of three additional Bulgarian authors are appropriate to our discourse. The first, Prof. Tzvetan Semerdjiev, published *Information War* in 2000. In a comprehensive manner he examined risks and threats to national security at the doorsteps of the 21st century, emphasizing those resulting from the proliferation of information technologies and communication channels. He introduced the concept of "national information space" and reasoned that defense should be organized in a number of echelons. Prof. Semerdjiev made detailed studies of the concept of information power, and applied the classic principles of warfare to elaborate on the principles of information warfare and the utilization of advanced IT.

The second author is Colonel Mitko Stoykov, who in 2003 published a book on the meaning of the information revolution for terrorism, and the way in which we organize our security system. Colonel Stoykov—then assigned to the Situation Center of the Ministry of Defense—examined three recent concepts: cyberwar, information war, and netwar in a comparative study of primarily US sources. His chapter on information operations was based almost exclusively on US doctrine:

Joint Pub 3-13, J*oint Doctrine for Information Operations*; FM 100-6; and Joint Publication 6-0, *Doctrine for Communications System Support to Joint Operations.*

This was probably the last comprehensive treatment of the issue of information operations by a Bulgarian author, to date. The main reason is that while downsizing of the Bulgarian Armed Forces continued, Bulgaria became a Membership Action Plan (MAP) country after the NATO Washington Summit and then, at the 2002 NATO Prague summit, was invited to join NATO. On its path to NATO membership, Bulgaria had to cope with a variety of requirements; interoperability and the protection of classified information had the strongest impact on all information-related issues. In combination with other constraints, these requirements overwhelmed the force planning and management capacity of Bulgaria's defense establishment. Just one example is that all cited authors continued to work and publish intensely on defense issues, but with no one focused specifically on information operations.

Most recently, Brigadier General Boyko Simitchiev—Chief of the Communications and Information Systems Directorate (J6) of the General Staff of the Bulgarian Armed Forces and Chief Information Officer for the defense establishment—contributed a paper to the journal *CIO.bg* that again raises interest in IO. In his opening statement he emphasized that the challenges of future war—and information operations in particular—will have a very important impact on the generation of requisite capabilities of the Bulgarian Armed Forces for participation in NATO and European Union missions. Without referring explicitly to the evolving concept of effects-based operations, he underlined the importance of achieving information superiority, and psychological operations' place in gaining the support of the local population. While developing capabilities to conduct information operations, we need to study the stability of our own systems performance against information attacks. In his conclusions, he emphasizes that in the near future the Bulgarian military must be able to plan and to participate in the conduct of information operations.

A novel element in General Simitchiev's paper was recognition of cyberspace as not only the place for military and governmental information operations, but also by terrorist organizations. Extremists aim to recruit members, disseminate propaganda, videos, brochures, and training materials, as well as to coordinate terrorist acts in an anonymous and interactive form. Echoing General Mihov, Simitchiev stated that cyberspace creates opportunities for spying, asymmetric impact, and propaganda that may lead to winning wars. Therefore, the next part examines approaches to countering use of cyberspace, and the Internet in particular, by terrorist and other extremist organizations.

General Zlatan Stoykov, Bulgarian Chief of Defence with Lieutenant General Atanas Zaprianov, Bulgarian Military Representative to the NATO Military Committee (NATO)

Bulgaria's Approach to Countering Extremists' Use of the Internet

With the amendment of military doctrine in the aftermath of September 11th, the Bulgarian Armed Forces were tasked by the legislature to contribute to anti- and counter-terrorism activities. However, an examination of Bulgaria's legislative framework on terrorism shows, by and large, this is a breach of law. Law enforcement organizations have the primary role in countering terrorism. This also applies to terrorist and extremist used of Internet, for a variety of purposes.

The Ministry of Interior in Bulgaria's executive branch is responsible for law enforcement. It includes three national services: Police, Security (counterintelligence), and Fire Safety and Protection of the Population.

The first organization that plays a role in countering extremist use of the Internet is the one dealing with organized crime. The National Service Police are tasked to counter criminal activities of local and cross-border criminal groups or organizations, to prevent terrorist acts, and to neutralize terrorist and diversion groups. Its Chief Directorate for Combating Organized Crime (CDCOC), with units in the Regional Police Directorates, "carries out independently or jointly with other specialized bodies operation and search activities of an informational and organizational nature to combat organized crime" related, among other things, to:

- Monetary, crediting, and financial systems
- Terrorist activities
- Computer (or cyber) crime
- Intellectual property rights

Second, fighting terrorism and extremism is among the main tasks of the National Security Service. This civilian counterintelligence activity identifies and neutralizes destructive processes that threaten constitutional order, the unity of the nation, and its sovereignty and territorial integrity. It also counters international terrorism and extremism.

Recently the Bulgarian Government announced plans for a major reorganization of its security agencies through the creation of a "National Agency for Security." The new agency unites three organizations: the National Security Service (currently under the

Bulgaria in its southeastern European context. (www.info.bg)

Ministry of the Interior); the Security Service (Military Counterintelligence) under the Ministry of Defense; and the Financial Intelligence Service (currently under the Ministry of Finance), and to place them under direct control of the Council of Ministers. This measure will raise the effectiveness and the efficiency of the fight against terrorism, organized crime, and crime at the 'high floors of power,' e.g. high-profile corruption.

A third realm of IO-related activities is protection of critical infrastructure, and in particular critical information infrastructure. Organizational developments in that respect are rather complex, and will not be examined in detail here. We only note that Bulgaria, as a member of the European Union since January 2007, adheres to EU Critical Infrastructure Protection (CIP) policies in particular as related to the fight against terrorism.

Accounting for the trans-border nature of crimes, aimed at or facilitated by the Internet, Bulgarian documents consistently express the readiness of the country for international cooperation, in particular in the framework of NATO and the European Union, but also in the expanding network of partnerships of these alliances and on a bilateral basis.

From a legislative point of view, a decree issued in the aftermath of September 11th prohibited any form of assistance—active or passive—to organizations and persons involved in terrorist acts, including efforts to recruit members of terrorist organizations.

Curiously however, the first cases against cyber crime involved breaches of intellectual property rights, and the illegal dissemination of software through the Internet. In those efforts, CDCOC joined forces with the Bulgarian Office of Business Software Alliance (BSA) that protects copyrights of software producers. BSA's influence was so strong that, according to a recent article in the newspaper *Capital*, the CDCOC unit tasked to fight cybercrime is "to a considerable degree modeled after the BSA views." The same article claims that the Ministry of the Interior orders Internet providers to block access to certain websites, i.e., to filter access to information.

The respective articles in Bulgaria's Penal Code form the legislative basis for such actions. Finally, the law on protection of classified information and related additional regulations prescribe principles and a complex set of measures for the prevention of unauthorized access to classified information created, processed, stored, and transported in automated information systems and networks.

Capability Management Challenges & Possible Developments

Any novel concept of operations is of practical importance only if incorporated in defense planning and force development processes. Furthermore, implementation of any information operations approach hangs on proper definition and development of respective capabilities.

Briefly summarized, in capabilities-based planning, required capabilities are defined against tasks to be performed under specified conditions, and requirements to produce concept-driven effects. For this purpose required effects are decomposed and matched with component capabilities. Then capabilities, at levels defined during the force planning process, are developed through the introduction of adequate procedures (or doctrine), organization, personnel policy, training, and technologies.

The implementation of this planning approach is extremely challenging, especially in the period after the year 2000, when the Bulgarian Armed Forces were downsized, and at the same time had to meet diverse interoperability requirements while sustaining its participation in Iraq, Afghanistan, Bosnia, and Kosovo operations. Bulgaria was even called upon to expand such participation in both its number of operations, and the numbers of soldiers deployed.

This combination of factors caused the relative decline of Bulgaria's efforts to further develop concepts of information operations and, more importantly, capabilities to participate in such operations. Nevertheless, during the past decade the Bulgarian defense establishment reached a certain level of conceptual and doctrinal maturity, assigning main IO responsibilities to military organizations, launching an ambitious program for the introduction of advanced communications and information technologies and, most importantly, gaining operational experience.

The main challenge at this stage is to promote information operations requirements among all competing requirements, and to elaborate realistic IO policies and an efficient capability development plan. These must also account for NATO and EU policies and burden sharing arrangements, as well as for developments in the national security sector. It is fairly safe to make several predictions in that respect:

First, the development of unique IO concepts as a result of original thinking, and in particular the implementation of such concepts, would hardly be encouraged. Instead, the Bulgarian military will adhere to the NATO military policy on information operations and information operations doctrine, as well as the EU concept for military IO. Nevertheless, it is important to underline that Bulgaria has the potential and willingness to contribute to NATO and EU IO-related research efforts, concept development and experimentation, or innovative developments in other bilateral or multinational forums.

Second, when it comes to the contribution to allied or coalition operations, one should not expect Bulgaria will develop and provide a broad spectrum of IO capabilities. Possibly the country will select a subset of capabilities, and will specialize in their development and utilization. In this respect, define generic units that are relatively self-sustained and can bring useful capabilities into a multinational operation is a topic of particular research interest.

Third, the IO attack aspect will most probably be subordinated to the evolving effects-based approach to operations (EBAO). Bulgaria will contribute to the development of this concept in the framework of NATO.

Finally, while protection of one's own command and control is part of defensive information operations, other elements of the information infrastructure may also be of considerable importance for the security of the state and society. As mentioned above, Bulgaria adheres to the EU policy on critical infrastructure protection and the major efforts will be on its implementation. At this stage the EU policy covers the Internet, but does not explicitly include defense or law enforcement infrastructure. It is still to be seen whether and how the military will cooperate with other governmental organizations and private actors in protecting critical national information infrastructure.

Conclusion

From 1995 till 2002, Bulgaria's interest in information operations was on the rise, but it has not been so prominent in the last five years. The decline in IO effort is relative—proponents find it very difficult to receive adequate financing among all competing requirements. The country still struggles to define areas of specialization within NATO and the EU in which Bulgaria wants to be competitive, and provide useful and efficient contributions. Nevertheless, it is possible to predict that Bulgaria will develop selective capabilities for conducting information operations as its contribution to the EBAO. The participation of the Bulgarian military in critical information infrastructure protection (CIIP) is less clear at this stage. The CIIP policy will reflect the policy of the European Union, with civilian organizations and the private sector in the lead. Whatever the decision, Bulgaria still needs a more realistic policy, and efficient capability management accounting, to meet developments in NATO, the European Union, and the national security sector.